eForensics Magazine

COMPUTER

FORENSIC FALCON

An experts Review

Logicube®

May ISSN 2300-6986

FORENSIC FALCON AN EXPERTS REVIEW

by ApoGeek

The first technical phase of a digital forensics investigation consists in acquiring evidence. The acquisition process for a computer that is powered off aims at creating an exact copy of the storage devices and peripherals. It must include all information required to enable the reconstruction of the structure and data of the given media device. As already detailed in previous eForensics Magazine articles, a low level bit-by-bit copy of the original physical device is deemed as the best method for achieving an (almost) perfect copy.

This article aims at providing some feedback on a recent test performed with the Forensic Falcon™ – from Logicube – while harvesting data spread over with multiple types of peripherals in a test bed environment. It follows the formal process of a first time responder or digital forensic investigator from opening the product's box, to analyzing the results it provides. The final part delivers some feedback and additional thoughts. All steps and actions that can be performed are not mentioned to cast more light on items of interest.

CONTEXT

Forensic examination of digital evidence must follow a repeatable and verifiable process that protects the integrity of original evidence and renders it unchanged. Using a tool that complies with that requirement is of utmost importance. Among all those available on the market, the question is to decide which one is the best? There are multiple criteria, including price, but the real ones are: are the features boasted in the data sheet true and properly implemented? How efficient are they? Is there any baseline? In our current case, the question must be split in 2 parts. First, what is a low level bit-by-bit copy? Second, how compliant are the tools?

Other open questions are related to the type of hardware drives that the forensic investigator will have to deal with, and the state of the drives. The integrity of the computer itself may not have been kept and it may have suffered from being partially burnt or dropped and broken, spoilt with a liquid... The availability of the right connector and their quality is another one.

Last but not least, an evidence may bear digital information in various formats: easily accessible but scrambled – e.g. compressed or encrypted – or password-protected, or worse, less easy to access and grab as it may have been in free space, deleted, partially wiped, or hidden. In any case, all attempts should be made to render the digital information as a viewable image that will be kept as a reference, and named "initial image". Any subsequent examination must be performed on additional copies of the initial image. So a low level bit-by-bit copy is a process often performed multiple times, and it has to be perfect.

Software Write-Blocking (SWB) solutions and Hardware Write-Blocking (HWB) devices both have pros and cons, the latter being preferred in many but not all cases. The correctness of the copy must be checked by using one or more algorithms to verify the initial image's integrity and authenticity.

Forensic imaging products play a critical role, they must deliver what they are supposed to deliver and … their users must know how to use it the right way. It may seem obvious but documentation must not be disregarded. First responders may not have technical background and will need a written procedure to follow strictly: the more user-friendly the user interface is, the better. For skilled digital forensic investigators, this may be less of an issue, but technical details and advanced user operations description will be a bonus.

OPENING THE FALCON BAG

The first responders and investigators must bring with them the appropriate hardware disk interfaces and all additional disk drives where the data will be copied. In real-life, it means having one or more bags with all hardware.

The bag supplied for the Falcon device offers good protection. It is both convenient and big enough to offer spare room for any additional hardware such as disk drives. All cables and accessories are supplied for the supported interfaces (see table).

The device itself only weights 1,2 kg thanks to a solid plastic outer case. However, the external power converter (12V, 12/5A) is a heavy one as it weights an extra 0.8 kg. But there is a good reason for that: it is required due to the large number of hard drives that can be connected to the Falcon at one time.

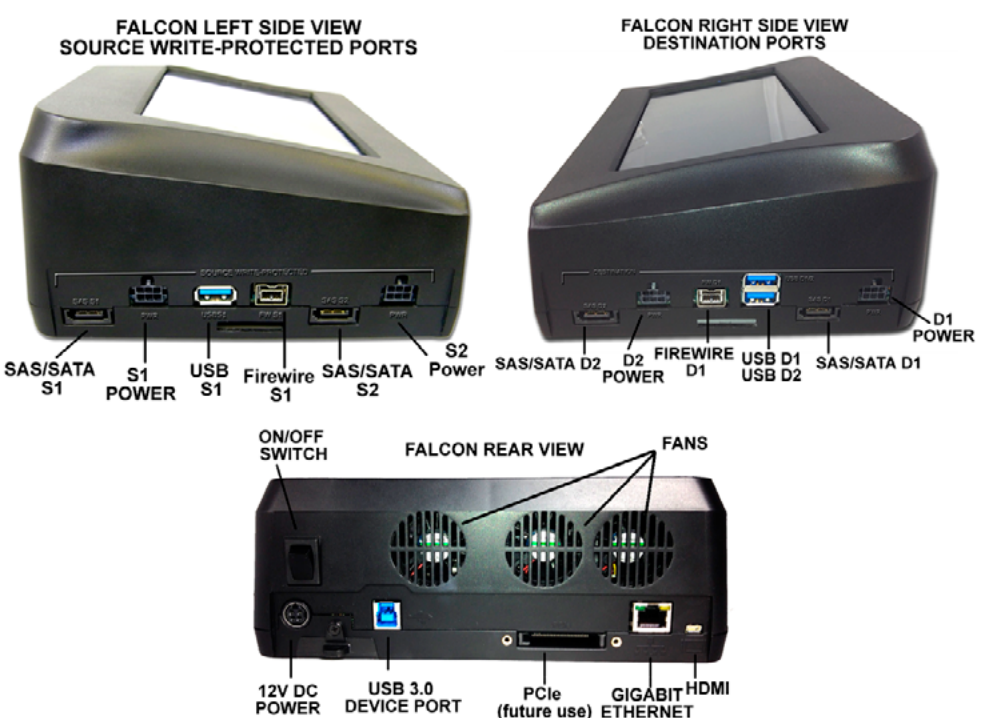
The Falcon takes 60% less space than the Logicube Dossier and measures 26.9cm X 21.6cm X 7.6cm. The physical access to the interfaces is easier too, and splitting the source and destination interfaces is also an improvement.

FALCON supported imaging ports		
	Source ports	Destination ports
SAS/SATA (1)	2	2
USB 3.0 (2)	1	2
Firewire	1	1
SCSI (3)	1	1
1.8"/2.5"/3.5" IDE and 1.8" IDE ZIF and microSATA interfaces are also supported with adapters. Optional adapters are available for eSATA, mSATA and flash drives.		
(1) with related power ports (2) can be converted to SATA using an optional USB to SATA adapter (3) using the SCSI Module Option		

Just looking at the device makes anyone understand its organization:

- A 7'' color-capacitive touch-screen interface on top;
- 2 USB host ports on the front;
- Write-protected source ports on the left;
- Destination ports on the right
- A USB 3.0 device port, a network interface with a built-in Gigabit Ethernet port, an HDMI port, the DC power and on/off power switch, and 3 openings for powerful fans.

The design team delivered a product easier to use.



A CDROM is also supplied. It includes the user's manual in PDF format, a 120 pages thick document with a well detailed table of contents, pictures and good explanations that even a non-technical responder will understand and enable him to use the device.

There is also a network interface which can be used to remotely access the device across a network, as well as perform the acquisition phase remotely. This opens up a new way to use the Falcon devices: start by deploying them at various sites to speed up the acquisition phase of targets spread all around a company or in subsidiaries.

So far, so good!

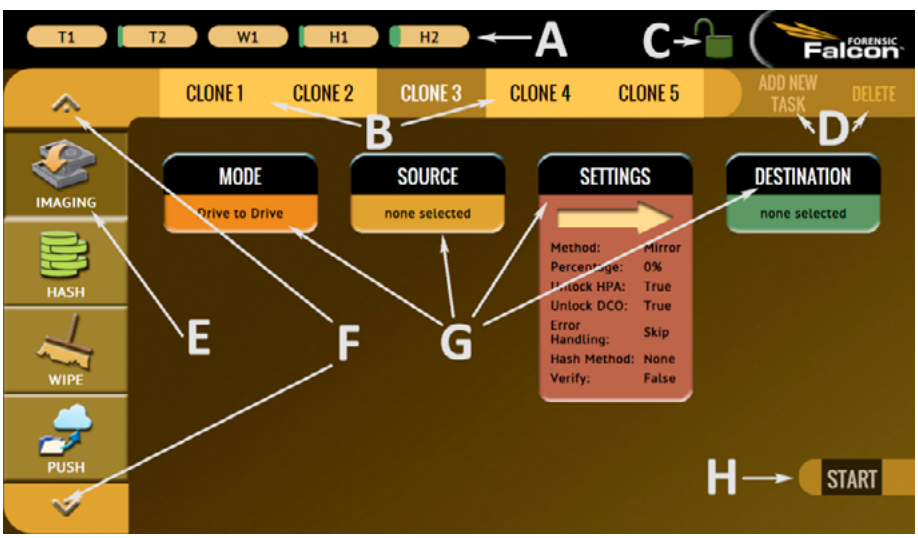
POWERING ON THE FALCON DEVICE

To turn on the FALCON device, just press the ON/OFF switch once, and the boot process starts right away. Fans start roaring, then the boot process can be seen on the screen and the whole process is finished, within 54 seconds. The level of noise generated by the fans will stay the same until the device is switched off.

The user interface is clean and the touch screen is responsive. For investigators with very big fingers or working is specific conditions, it is possible to use a stylus as with any tablet or PDA. It is also possible to connect a mouse to one of the USB ports.

The Falcon device uses a Linux-based Ubuntu operating system, as it can be understood from the FAQ and the documentation. Multitasking enables the user to perform more than one scenario at the same time to speed up the process and run operations in parallel. Moreover, sessions can be saved and put in a library. Once again, automation and remote operations capabilities come to the mind. Re-running pre-defined sessions prevents errors, and may greatly help demonstrate and validate the evidence collection process in a court. For an analyst working on multiple instances of evidences, this is also a guarantee that the evidence collection process has been performed the same way, whatever the location or the technical knowledge of the first responder is.

Back to the user interface, the left side of the screen lists the 13 different types of operation available in a column. These types are: imaging; hash; wipe; push; task macros; USB device (viewing drive contents in Windows); logs (that can be protected with a local password, as well as accessed remotely); statistics (Falcon and drive statistics); manage repositories; system settings; IP settings (proxy settings); software updates; and power off.



A – Operations/Tasks currently running
B – Operations/Tasks
C – Lock indicator/shortcut
D – Add or delete tasks
E – Types of Operations
F – Up and down scroll arrows
G – Operations options and settings
H – Start icon

The last one is a software “power off” operation which allows to softly turn off the device, which happens in a few seconds. A soft switch performing a clean shutdown of a Linux system is always our preferred action, as we have seen in the past the negative effect of a hard “power off” switch.

FIRST ACTION

Before starting a low level bit-by-bit copy of an original physical device, it is better to have a clean and reliable destination disk drive. The best way to achieve this goal simply is to use the “Wipe” operation of the Falcon itself. It features 3 methods:

- "Secure Erase" that will issue a command to the disk drive to perform a wipe action based on the hard drive manufacturer's specifications;
- "Wipe Patterns" that allows the user to set a specific pattern to use for wiping the drive, with a customizable number of passes (up to 7) along with the type of data written for each pass.
- "Format" which will format a disk drive using the EXT4 file system or NT file system (NTFS).

All three actions are efficient and tests to check the quality of the actions are positive. All three can be performed without any forensics knowledge and can be delegated to forensics operators for massive campaigns.

Two cases are worth noting:

- The Falcon "format" converts any non-POSIX portable characters [1] used in Case/File Name field to underscores "_" when creating the log or file names;
- If the drive has a Host Protected Areas (HPA) or Device Configuration Overlay (DCO) area that needs to be wiped, it can be: it just needs to be explicitly configured.

So the task is easy to perform. It is useless to ask about performance, as the tests performed showed that the key factor is the peripheral characteristics rather than the Falcon device itself.

So we now have a FALCON device ready, and a clean spare disk.

MANUAL COPY

The first manual tests performed were the simple disk copying. Needless to say, a basic function is expected to be performed without a hitch. This is the case: configuring the imaging process is simple and has 3 flavors: drive-to-drive, file-to-file, and drive-to-file.

The first 2 are obvious, and enable the user to blindly copy large chunks of data, granted that the destination is large enough. The settings for the imaging process include a few parameters or fields such as a comment to detail the forensics case, the HPA/DCO clone setting, the important error handling behavior that either enables to skip the bad sectors or to abort the process, and the hash and verification methods (MD5, SHA-1, SHA-256). Interestingly, it is possible to only mirror parts of a drive.

The drive-to-drive performs as expected, literally: however large the destination container is, it is an exact copy of the source drive. As an example, copying a 8GB USB stick on a 1TB disk can make it appear like a 8GB USB stick too!

This is where the third option comes into line: the capability to copy multiple sources to a single receiving drive as images. This is the most common case in real-life digital investigations, hence the one to be preferred. The 3 image output file formats are: plain DD [2], or compressed [3] or uncompressed E01, and EX01 [4]. And when the destination container is full, just ask! The Falcon device can automatically span to at least 2 destination containers in the “Drive-to-File” mode. When the first one becomes full, the user interface of the device prompts to replace the existing container by a new one to fit the remaining data to be imaged.

So far, so good, except that in the most digital investigations, time is a critical factor: locating and collecting huge amount of data translates into hours – if not days – of work, as peripherals contain increasing volumes of disk spaces. In order to spare time and get some control over the time it may take, the digital investigator must sort out and select the right data to preserve.

Haste makes waste! This is a long process that requires integrity and quality. Integrity translates into verification, and verification is an additional process that increases the amount of time required. “*To hash or not to hash, that is the question*!”.

Fortunately, the throughput of the Falcon device is really impressive, and in our tests, the destination disk drives proved to be the limitation to performance. The Falcon datasheet boasts a “fast forensic imaging at 20GB/min”, but this figure could not be reached, as the required resources were not available in the lab where the tests were performed.

Fast access disk drives is one mitigation path. Another one is using an additional function of the device, as it is much more powerful than the source(s) to be copied: parallel imaging. The tests did not showed any speed difference compared to single tasking, hence it did not affect the performance of the Falcon device.

The parallel imaging is definitely an option to study when confronted with huge amount of data to deal with. Another option is to use the patent-pending “Concurrent Image+Verify” feature on the device.

This is a unique feature that really addresses the need for investigators to shorten the entire evidence collection process. Instead of first imaging the entire drive and then performing a read/verify of the drive, imaging and verifying take place simultaneously and takes advantage of fast destination hard drives that may be faster than the source hard drive. Duration of total image and verify process time may be reduced by up to half depending on the speed of the destination in relationship to the speed of the source.

It should be noted that another mode has not been tested during the lab experiment due to internal logistical issues: copying/imaging over a network from or to a remote device. But based on the information supplied in the manual of the device, the network option is also worth considering.

As a conclusion to the imaging process, it works as expected and embeds some additional nice features. When short of time the following saying will apply to the destination disk drive: “the faster, the better”.

AUTOMATION

One of the nicest features of the device is not a technical one, but one that relates to usage: ease of use. For one, the user interface is nice and user-friendly as already mentioned. When it comes to organization and team handling, splitting tasks between various stakeholders is a key element.

The door to automation and delegation of tasks is being opened on the Falcon device by what is named “Task Macros”. Up to 5 “macros” of up to 9 “operations” or single actions such as cloning, hashing, pushing, and wiping. The configuration process is easy: it is exactly the same as with manual operations, each task being configured one after the other, and the list of operations are then recorded. Once done, it shows up in the list of “Macros”, and a new one can be created.

For recurring activities with the device, mass cloning or when the device must be shipped to a remote location without any trained operator, this is a good solution. It just requires you to write a simple procedure that details all steps from unpacking the device, to inserting the items in the appropriate source ports on the device, and selecting the appropriate macro. This feature has at least 3 advantages:

- It saves time by eliminating the need to write a procedure that describes all the technical steps;
- It lowers the risk of misunderstanding from the operators' side, and prevents human errors as all technical steps are tested and predefined;
- It enables to have a library of validated processes so that all sorts of users with varying levels of expertise are able to perform standardized tasks around digital evidence gathering.

OTHERS FEATURES

A few more features are available with the Falcon device:

- The network "Push" feature that enables to send evidence to the device, or from the device to a remote network repository, with data integrity being checked while the data is transferred;
- Various configuration can be configured to take into account the context and the usage of the Falcon device: passwords, systems settings (language: English or Korean; encryption...) or network ones (remote repository, network proxy...). A repository can be accessed using the iSCSI protocol, but this has not been tested in our lab. In all network configurations, password can be attributed and are kept within the device;
- Logs are created for any action launched on the device (imaging, hashing, wiping, formatting, and pushing), and can be kept secured by password-protecting them;
- Privacy can be enforced with what Logicube names the "Stealth mode" which keeps the screen off, so none can guess what is going on.

Password can also be used in the deployment configuration, to keep the logs secured and prevent any tampering. The same applies to the configuration which can be frozen and cannot be changed by any local stakeholder. Once shipped the device can only be used the way it was thought, and this will bring peace of mind to the digital investigation project manager: tasks can be started, but they cannot be modified.

The documentation includes a chapter entitled "Drive Encryption and Decryption" which explains how to use encrypted media as output. It is then possible to use one Falcon device for collecting evidences, encrypt the media with a given secret at the device level, and ship it, in order to lower the risks of tampering. Once at destination, the media can be decrypted with the secret. This can be done using another Falcon device, or interestingly, decryption can even be performed on a Windows-based platform using either the well-known TrueCrypt [5] or FreeOTFE.

The tests performed with TrueCrypt proved to be positive. The 3 pre-requisites were: to define the receiving media as a formatted encrypted container; to configure the encryption settings at TC-XTS, and AES-256; and then to format the media as an NTFS partition.

The media must be mounted as a "device" in TrueCrypt in order gain access to the encrypted part. Then it works perfectly, it is another nice feature of the product: interoperability. A typical scenario is where the acquisition phase is done by rank and file evidence collection agents who must then send the evidence media to a digital investigator. Using TrueCrypt as an added encryption layer makes sense. Do keep in mind that apart from Windows, TrueCrypt has been ported to Mac OS X and Linux, and even to Android. In case a forensics investigation requires a higher level of more segmentation, this may well be used.

Once again, in case of a secure deployment, this is an option to look for, with encryption being part of the chain of custody.

CONCLUSION

Apart from the 2 minor issues that are related to the power supply weight and the noisy fans, the pros are obvious:

- The user interface is really a user-friendly one;
- The implemented functionalities are both useful and do perform as expected;
- The Scripting/Macro language and automation capabilities are enabling;
- The technical tests that have been performed have all been successful;
- Speed and performance are there;
- Care taken to protect the exchanges from a confidentiality and integrity standpoint;
- The packaging is well suited and all cables are supplied with the Falcon device.

To finish with, the documentation provides useful guidance, and hints: we did not have to call the support to get any sort of help during the test. The configuration of the various parameters proved to be satisfactory and the copy, wipe and format options were the ones that may be necessary in most, if not all, digital investigations in the field. At the techie level, fits in for the job and turned to be above expectations.

We also wanted to get the point of view of non-security specialists. We gave IT staff with no knowledge on forensics a written procedure with simple tasks to perform, and handed them over the Falcon device. Starting from scratch and discovering the user-interface, they were easily able to perform the requested tasks.As a conclusion, we believe the Falcon device is an excellent product, with robust features, and a user-friendly interface. All in all, this is the type of product that we can highly recommend that digital investigators add to their set of tools.

REFERENCES

[1] POSIX portable characters are: Uppercase “A” to “Z”, Lowercase “a” to “z”, Numbers “0” to “9”, Period “.”, Underscore “_”, Hyphen/Dash “-”
[2] “DD” format is uncompressed raw image files that can be read by most forensic programs.
[3] Compression strength can be tuned with a slider bar on the user interface.
[4] “E01” and “EX01” are compressed or uncompressed EnCase legacy evidence file formats.
[5] The famous free open-source encryption software is available at *http://www.truecrypt.org/*

ABOUT THE AUTHOR

ApoGeeK has been working as a security guy for over 20 years, starting as a network security expert.
He has worked extensively on network attacks, network forensics and analysis, than came to the systems world with Windows, and Unix/Linux. He has worked on cybercrime cases as well as APT attacks.
He has used both Software Write-Blocking (SWB) solutions and Hardware Write-Blocking (HWB) ones.

LogiCube®